Lecture 21

Cellular Networks Security

This work is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License.
Lecture 21—Contents

2nd generation cellular networks: GSM

3rd generation cellular networks: UMTS

4th generation cellular networks: LTE

5th generation cellular networks
GSM reference architecture
GSM security fundamentals

Security services

GSM security was designed to provide the following services:

- User privacy against attackers trying to identify and/or trace a specific user's location
- Access control against network usage by unauthorized entities
- User authentication against billing frauds
- User data secrecy against eavesdropping on the radio channel

Long term credentials

The long term credentials for a user A are his/her International mobile subscriber identity (IMSI) and his master secret key $k_A$. The pair $(id_A, k_A)$ is stored in the user owned Subscriber identity module (SIM) and in the corresponding Authentication center. 

Nicola Laurenti

Cellular Networks Security
## GSM security fundamentals

### Security services

GSM security was designed to provide the following services:

- **User privacy** against attackers trying to identify and/or trace a specific user’s location
- **Access control** against network usage by unauthorized entities
- **User authentication** against billing frauds
- **User data secrecy** against eavesdropping on the radio channel

**Long term credentials**

The long term credentials for a user $A$ are his/her International mobile subscriber identity (IMSI) $A$ and his master secret key $k_A$. The pair $(id_A, k_A)$ is stored in the user owned Subscriber identity module (SIM) and in the corresponding Authentication center.
# GSM security fundamentals

## Security services

GSM security was designed to provide the following services:

- **User privacy** against attackers trying to identify and/or trace a specific user’s location
- **Access control** against network usage by unauthorized entities
- **User authentication** against billing frauds
- **User data secrecy** against eavesdropping on the radio channel

Long term credentials:

The long term credentials for a user $A$ are his/her **International mobile subscriber identity (IMSI)** and his **master secret key** $k_A$. The pair $(\text{IMSI}_A, k_A)$ is stored in the user owned **Subscriber identity module (SIM)** and in the corresponding **Authentication center**.
GSM security fundamentals

Security services

GSM security was designed to provide the following services:

- **User privacy** against attackers trying to identify and/or trace a specific user’s location
- **Access control** against network usage by unauthorized entities
- **User authentication** against billing frauds

Long term credentials

The long term credentials for a user A are his/her International mobile subscriber identity (IMSI) and his master secret key. The pair \((\text{IMSI}_A, k_A)\) is stored in the user owned Subscriber identity module (SIM) and in the corresponding Authentication center.
GSM security fundamentals

Security services

GSM security was designed to provide the following services:

- **user privacy** against attackers trying to identify and/or trace a specific user’s location
- **access control** against network usage by unauthorized entities
- **user authentication** against billing frauds
- **user data secrecy** against eavesdropping on the radio channel

Long term credentials

The long term credentials for a user A are his/her International mobile subscriber identity (IMSI) and his master secret key $k_A$. The pair $(id_A, k_A)$ is stored in the user owned Subscriber identity module (SIM) and in the corresponding Authentication center.
GSM security fundamentals

Security services

GSM security was designed to provide the following services:

- **User privacy** against attackers trying to identify and/or trace a specific user’s location
- **Access control** against network usage by unauthorized entities
- **User authentication** against billing frauds
- **User data secrecy** against eavesdropping on the radio channel

Long term credentials

The long term credentials for a user A are his/her *International mobile subscriber identity (IMSI)* $\text{id}_A$ and his *master secret* key $k_A$.

The pair $(\text{id}_A, k_A)$ is stored in the user owned *Subscriber identity module (SIM)* and in the corresponding *Authentication center*. 
GSM security design principles

- protection of the (mobile – base station) radio link only

- completely new cryptographic functions (not publicly discussed before standardization)

- non mutual entity authentication: only the mobile user is authenticated

- interactive authentication protocol to be performed between mobile and visited BSC

- long term credentials are not shared with the visited BSC (may belong to another operator)

- assignment of a temporary pseudonym to mobile

- low complexity encryption / decryption
GSM security design principles

- protection of the (mobile – base station) radio link only
- completely new cryptographic functions (not publicly discussed before standardization)
GSM security design principles

- protection of the (mobile – base station) radio link only
- completely new cryptographic functions (not publicly discussed before standardization)
- non mutual entity authentication: only the mobile user is authenticated
GSM security design principles

- protection of the (mobile – base station) radio link only
- completely new cryptographic functions (not publicly discussed before standardization)
- non mutual entity authentication: only the mobile user is authenticated
- interactive authentication protocol to be performed between mobile and visited BSC
GSM security design principles

- protection of the (mobile – base station) radio link only
- completely new cryptographic functions (not publicly discussed before standardization)
- non mutual entity authentication: only the mobile user is authenticated
- interactive authentication protocol to be performed between mobile and visited BSC
- long term credentials are not shared with the visited BSC (may belong to another operator)
GSM security design principles

- protection of the (mobile – base station) radio link only
- completely new cryptographic functions (not publicly discussed before standardization)
- non mutual entity authentication: only the mobile user is authenticated
- interactive authentication protocol to be performed between mobile and visited BSC
- long term credentials are not shared with the visited BSC (may belong to another operator)
- assignment of a temporary pseudonym to mobile
GSM security design principles

- protection of the (mobile – base station) radio link only
- completely new cryptographic functions (not publicly discussed before standardization)
- non mutual entity authentication: only the mobile user is authenticated
- interactive authentication protocol to be performed between mobile and visited BSC
- long term credentials are not shared with the visited BSC (may belong to another operator)
- assignment of a temporary pseudonym to mobile
- low complexity encryption / decryption
GSM mobile user authentication protocol

```
mobile terminal M  visited base station V  auth center H
```

1. **M** \(\rightarrow\) \(V\): id \(M\), id \(H\)

2. **V** \(\rightarrow\) **H**: id \(M\), id \(V\)

3. **H**: for \(n = 1, \ldots, N\):
   - generate random challenge (128 bit) \(c_n \sim U(C)\)
   - compute expected response (32 bit) \(\hat{r}_n = A_3(k_M, c_n)\)
   - compute session key (64 bit) \(\hat{k}'_n = A_8(k_M, c_n)\)

4. **H** \(\rightarrow\) **V**: \([c_1, r_1, k'_1, \ldots, c_N, r_N, k'_N]\)

5. **V** \(\rightarrow\) **M**: \(c_1\)

6. **M** \(\rightarrow\) **V**: \(r_1\)

If \(\hat{r}_1 = \hat{r}_1\), accept \(M\) and generate temporary id \(\tilde{id}_M\), \(1\)

**V** \(\rightarrow\) **M**: \([id_V, id'_M, 1]\)

Nicola Laurenti
Cellular Networks Security
GSM mobile user authentication protocol

1. $M \rightarrow V : id_M, id_H$

- Mobile terminal
- Visited base station
- Authentication center

Diagram:

- Mobile terminal $M$
- Visited base station $V$
- Authentication center $H$

Steps:
1. $M \rightarrow V : id_M, id_H$
2. $V \rightarrow M : r_1$
3. $M \rightarrow V : c_1, r_1, k'_1$
4. $V \rightarrow M : [id_V, id'_M]$

Session key calculation:
- $k'_1 = \text{A}_8(k_M, c_1)$
- $r_1 = \text{A}_3(k_M, c_1)$

Authentication process:
- If $\hat{r}_1 = \hat{r}_1$, accept $M$ and generate temporary $id'_M$. 

Nicola Laurenti

Cellular Networks Security

December 5, 2017
GSM mobile user authentication protocol

1. M → V: id_M, id_H
2. V → H: id_M, id_V
GSM mobile user authentication protocol

1. M → V : id_M, id_H
2. V → H : id_M, id_V
3. H : for n = 1, ..., N:
   - generate random challenge (128 bit) c_n ~ U(C)
   - compute expected response (32 bit) \( \hat{r}_n = A_3(k_M, c_n) \)
   - compute session key (64 bit) \( \hat{k}_n' = A_8(k_M, c_n) \)
4. H → V : [c_1, r_1, k_1', ..., c_N, r_N, k_N']
**GSM mobile user authentication protocol**

1. M → V: id_M, id_H
2. V → H: id_M, id_V
3. H: for n = 1, ..., N:
   - generate random challenge (128 bit) \( c_n \sim U(C) \)
   - compute expected response (32 bit) \( \hat{r}_n = A3(k_M, c_n) \)
   - compute session key (64 bit) \( \hat{k}'_n = A8(k_M, c_n) \)
4. H → V: \( [c_1, r_1, k'_1, \ldots, c_N, r_N, k'_N] \)
5. V → M: \( c_1 \)
2nd generation cellular networks: GSM

GSM mobile user authentication protocol

- Mobile terminal: $M$
- Visited base station: $V$
- Auth center: $H$

1. $M \rightarrow V$: $id_M, id_H$
2. $V \rightarrow H$: $id_M, id_V$
3. $H$: for $n = 1, \ldots, N$
   - generate random challenge (128 bit) $c_n \sim \mathcal{U}(C)$
   - compute expected response (32 bit) $\hat{r}_n = A3(k_M, c_n)$
   - compute session key (64 bit) $\hat{k}'_n = A8(k_M, c_n)$
4. $H \rightarrow V$: $[c_1, r_1, k'_1, \ldots, c_N, r_N, k'_N]$
5. $V \rightarrow M$: $c_1$
6. $M$: compute response $r_1 = A3(k_M, c_1)$
   - compute session key $k'_1 = A8(k_M, c_1)$
7. $M \rightarrow V$: $r_1$
GSM mobile user authentication protocol

1. M → V : \(\text{id}_M, \text{id}_H\)
2. V → H : \(\text{id}_M, \text{id}_V\)
3. H : for \(n = 1, \ldots, N\):
   - generate random challenge (128 bit) \(c_n \sim \mathcal{U}(C)\)
   - compute expected response (32 bit) \(\hat{r}_n = A3(k_M, c_n)\)
   - compute session key (64 bit) \(\hat{k}'_n = A8(k_M, c_n)\)
4. H → V : \([c_1, r_1, k'_1, \ldots, c_N, r_N, k'_N]\)
5. V → M : \(c_1\)
6. M : compute response \(r_1 = A3(k_M, c_1)\)
   - compute session key \(k'_1 = A8(k_M, c_1)\)
   - M → V : \(r_1\)
6. V : if \(\hat{r}_1 = \hat{r}_1\), accept M and generate temporary \(\text{id}'_{M,1}\)
   - V → M : \([\text{id}_V, \text{id}'_{M,1}]\)
GSM re-authentication protocol

With the same VLR V:

mobile terminal M

visited base station V

\[ M \rightarrow V: \text{id}^{\prime}M, n, \text{id}V \]

\[ V \rightarrow M: c_{n+1} \]

\[ M: \text{compute} r_{n+1} = A_3(k_M, c_{n+1}) \text{ and } k^{\prime}_{n+1} = A_8(k_M, c_{n+1}) \]

\[ M \rightarrow V: r_{n+1} \]

\[ V: \text{if} \hat{r}_{n+1} = \hat{r}_{n+1}, \text{accept M and generate temporary id}^{\prime}M, n+1 \]
GSM re-authentication protocol

With the same VLR V:

1. $M \rightarrow V : \text{id}^{'}_{M,n}, \text{id}_V$
GSM re-authentication protocol

With the same VLR V:

\[ \text{mobile terminal} \quad M \quad \rightarrow \quad V : \quad \text{id'}_{M,n}, \text{id}_V \]

\[ \text{visited base station} \quad V \quad \rightarrow \quad M : \quad c_{n+1} \]
GSM re-authentication protocol

With the same VLR V:

1. M → V: id'_{M,n}, id_V
2. V → M: c_{n+1}
3. M: compute \( r_{n+1} = A_3(k_M, c_{n+1}) \) and \( k'_{n+1} = A_8(k_M, c_{n+1}) \)

M → V: r_{n+1}
GSM re-authentication protocol

With the same VLR V:

1. $M \rightarrow V : \text{id}_{M,n}^{\prime}, \text{id}_V$

2. $V \rightarrow M : c_{n+1}$

3. $M : \text{compute } r_{n+1} = A_3(k_M, c_{n+1}) \text{ and } k'_{n+1} = A_8(k_M, c_{n+1})$
   $M \rightarrow V : r_{n+1}$

4. $V : \text{if } \hat{r}_{n+1} = \hat{r}_{n+1}, \text{ accept } M \text{ and generate temporary } \text{id}_{M,n+1}^{\prime}$
   $V \rightarrow M : [\text{id}_V, \text{id}_{M,n+1}^{\prime}]$
GSM re-authentication protocol

Handover from a VLR $V_1$ to another VLR $V_2$:

Mobile terminal $M$ → $V_2$

New base station $V_2$ → Previous base station $V_1$

Mobile terminal $M$ → $V_2$:

$\text{id}'_{M,n}, \text{id}_{V_1}$

New base station $V_2$ → Previous base station $V_1$:

$\text{id}'_{M,n}, \text{id}_{V_1}$

Previous base station $V_1$ → New base station $V_2$:

$\text{id}'_{M,n}, \text{id}_{M}, [c_{n+1}, r_{n+1}, k'_{n+1}, \ldots, c_{N}, r_{N}, k'_{N}]$

New base station $V_2$ → Mobile terminal $M$:

$c_{n+1}$

Mobile terminal $M$ computes:

$r_{n+1} = A_3(k_M, c_{n+1})$ and $k'_{n+1} = A_8(k_M, c_{n+1})$

Mobile terminal $M$ → New base station $V_2$:

$r_{n+1}$

New base station $V_2$: if $\hat{r}_{n+1} = \hat{r}_{n+1}$, accept $M$ and generate temporary $\text{id}'_{M,n+1}$

New base station $V_2$ → Mobile terminal $M$:

[$\text{id}_{V_2}, \text{id}'_{M,n+1}$]
GSM re-authentication protocol

Handover from a VLR $V_1$ to another VLR $V_2$:

1. $M \rightarrow V_2 : \text{id}'_{M, n}, \text{id}_{V_1}$
GSM re-authentication protocol

Handover from a VLR $V_1$ to another VLR $V_2$:

1. $M \rightarrow V_2 : \text{id}_{M,n}^{\prime}, \text{id}_{V_1}$
2. $V_2 \rightarrow V_1 : \text{id}_{M,n}^{\prime}, \text{id}_{V_1}$
GSM re-authentication protocol

Handover from a VLR $V_1$ to another VLR $V_2$:

1. $M \rightarrow V_2 : \text{id}'_{M,n}, \text{id}_{V_1}$
2. $V_2 \rightarrow V_1 : \text{id}'_{M,n}, \text{id}_{V_1}$
3. $V_1 \rightarrow V_2 : \text{id}'_{M,n}, \text{id}_M, [c_{n+1}, r_{n+1}, k'_{n+1}, \ldots, c_N, r_N, k'_N]$
GSM re-authentication protocol

Handover from a VLR V\(_1\) to another VLR V\(_2\):

1. \(M \rightarrow V_2\) : \(\text{id}_{M,n}', \text{id}_{V_1}\)
2. \(V_2 \rightarrow V_1\) : \(\text{id}_{M,n}', \text{id}_{V_1}\)
3. \(V_1 \rightarrow V_2\) : \(\text{id}_{M,n}', \text{id}_M, [c_{n+1}, r_{n+1}, k'_{n+1}, \ldots, c_N, r_N, k'_N]\)
4. \(V_2 \rightarrow M\) : \(c_{n+1}\)
GSM re-authentication protocol

Handover from a VLR $V_1$ to another VLR $V_2$:

1. $M \rightarrow V_2 : \text{id}'_{M,n}, \text{id}_{V_1}$
2. $V_2 \rightarrow V_1 : \text{id}'_{M,n}, \text{id}_{V_1}$
3. $V_1 \rightarrow V_2 : \text{id}'_{M,n}, \text{id}_M, [c_{n+1}, r_{n+1}, k'_{n+1}, \ldots, c_N, r_N, k'_N]$
4. $V_2 \rightarrow M : c_{n+1}$
5. $M : \text{compute } r_{n+1} = A3(k_M, c_{n+1}) \text{ and } k'_{n+1} = A8(k_M, c_{n+1})$
   $M \rightarrow V_2 : r_{n+1}$
GSM re-authentication protocol

Handover from a VLR $V_1$ to another VLR $V_2$:

1. $M \rightarrow V_2 : \text{id}_{M,n}^{'}, \text{id}_{V_1}$
2. $V_2 \rightarrow V_1 : \text{id}_{M,n}^{'}, \text{id}_{V_1}$
3. $V_1 \rightarrow V_2 : \text{id}_{M,n}^{'}, \text{id}_M, [c_{n+1}, r_{n+1}, k'_{n+1}, \ldots, c_N, r_N, k'_{N}]$
4. $V_2 \rightarrow M : c_{n+1}$
5. $M : \text{compute } r_{n+1} = A3(k_M, c_{n+1}) \text{ and } k'_{n+1} = A8(k_M, c_{n+1})$
   $M \rightarrow V_2 : r_{n+1}$
6. $V_2 : \text{if } \hat{r}_{n+1} = \hat{r}_{n+1}, \text{accept } M$
   and generate temporary $\text{id}_{M,n+1}^'$
   $V_2 \rightarrow M : [\text{id}_{V_2}, \text{id}_{M,n+1}^']$
GSM encryption

The A5/1 is a binary additive stream cipher, obtained by nonlinear combination of 3 LFSR ciphers. The state and the key are 64 bit long.
GSM security vulnerabilities

In the authentication protocol

- No authentication of V to M
- M will respond to any challenge
- Weakness of the A3 function: for some $c_n = \gamma_i$, $r_n$ leaks information about $k_M$
- A3 is used in a time invariant way
- A3 recovery attack
  - By simulating a fake base station in the vicinity of the victim mobile,
  - Or by directly accessing the victim SIM (phone resellers, repair shops, ...)
- An attacker can submit challenges $\{\gamma_i\}$ and recover $k_M$ (aka SIM cloning)

In the encryption mechanism

- State update of A5/1 is not one-to-one
- Long time with the same V, states will concentrate
- 64 bit key / state are too short
- Biased birthday state guessing attack
  1. precompute the 64-bit outputs that correspond to the most likely states
  2. observe until any of them appears in the actual transmission
GSM security vulnerabilities

In the authentication protocol

- No authentication of V to M $\Rightarrow$
- M will respond to any challenge

In the encryption mechanism

- State update of A5/1 is not one-to-one
- Long time with the same V, states will concentrate
- 64 bit key / state are too short
  - Biased birthday state guessing attack
  1. precompute the 64-bit outputs that correspond to the most likely states
  2. observe until any of them appears in the actual transmission
GSM security vulnerabilities

In the authentication protocol

- No authentication of V to M ⇒ M will respond to any challenge
- Weakness of the A3 function: for some $c_n = \gamma_i, r_n$ leaks information about $k_M$
GSM security vulnerabilities

In the authentication protocol

- No authentication of V to M $\Rightarrow$ M will respond to any challenge
- Weakness of the A3 function: for some $c_n = \gamma_i, r_n$ leaks information about $k_M$
- A3 is used in a time invariant way
2nd generation cellular networks: GSM

GSM security vulnerabilities

In the authentication protocol

- No authentication of V to M ⇒ M will respond to any challenge
- Weakness of the A3 function: for some $c_n = \gamma_i$, $r_n$ leaks information about $k_M$
- A3 is used in a time invariant way

$k_M$ recovery attack

- By simulating a fake base station in the vicinity of the victim mobile,
- or by directly accessing the victim SIM (phone resellers, repair shops, ...)

an attacker can submit challenges $\{\gamma_i\}$ and recover $k_M$ (aka SIM cloning)
2nd generation cellular networks: GSM

GSM security vulnerabilities

In the authentication protocol
- No authentication of V to M ⇒ M will respond to any challenge
- Weakness of the A3 function: for some $c_n = \gamma_i$, $r_n$ leaks information about $k_M$
- A3 is used in a time invariant way

$k_M$ recovery attack
- By simulating a fake base station in the vicinity of the victim mobile,
- or by directly accessing the victim SIM (phone resellers, repair shops, ...)

an attacker can submit challenges $\{\gamma_i\}$ and recover $k_M$ (aka SIM cloning)

In the encryption mechanism
- State update of A5/1 is not one-to-one
- Long time with the same V, states will concentrate
- 64 bit key / state are too short

Biased birthday state guessing attack
1. precompute the 64-bit outputs that correspond to the most likely states
2. observe until any of them appears in the actual transmission
GSM security vulnerabilities

In the authentication protocol
- No authentication of V to M ⇒ M will respond to any challenge
- Weakness of the A3 function: for some $c_n = \gamma_i$, $r_n$ leaks information about $k_M$
- A3 is used in a time invariant way

$k_M$ recovery attack
- By simulating a fake base station in the vicinity of the victim mobile,
- or by directly accessing the victim SIM (phone resellers, repair shops, ...)

an attacker can submit challenges $\{\gamma_i\}$ and recover $k_M$ (aka SIM cloning)

In the encryption mechanism
- State update of A5/1 is not one-to-one
GSM security vulnerabilities

In the authentication protocol
- No authentication of V to M ⇒ M will respond to any challenge
- Weakness of the A3 function: for some $c_n = \gamma_i$, $r_n$ leaks information about $k_M$
- A3 is used in a time invariant way

$k_M$ recovery attack
- By simulating a fake base station in the vicinity of the victim mobile,
- or by directly accessing the victim SIM (phone resellers, repair shops, …)

an attacker can submit challenges $\{\gamma_i\}$ and recover $k_M$ (aka SIM cloning)

In the encryption mechanism
- State update of A5/1 is not one-to-one
- Long time with the same V, states will concentrate
GSM security vulnerabilities

In the authentication protocol

- No authentication of V to M \( \Rightarrow \) M will respond to any challenge
- Weakness of the A3 function: for some \( c_n = \gamma_i, r_n \) leaks information about \( k_M \)
- A3 is used in a time invariant way

\( k_M \) recovery attack

- By simulating a fake base station in the vicinity of the victim mobile,
- or by directly accessing the victim SIM (phone resellers, repair shops, ...)

In the encryption mechanism

- State update of A5/1 is not one-to-one
- Long time with the same V, states will concentrate
- 64 bit key / state are too short

Nicola Laurenti
Cellular Networks Security
December 5, 2017
GSM security vulnerabilities

**In the authentication protocol**
- No authentication of V to M \( \Rightarrow \) M will respond to any challenge
- Weakness of the A3 function: for some \( c_n = \gamma_i, r_n \) leaks information about \( k_M \)
- A3 is used in a time invariant way

**\( k_M \) recovery attack**
- By simulating a fake base station in the vicinity of the victim mobile,
- or by directly accessing the victim SIM (phone resellers, repair shops, ...)
  
  an attacker can submit challenges \( \{\gamma_i\} \) and recover \( k_M \) (aka SIM cloning)

**In the encryption mechanism**
- State update of A5/1 is not one-to-one
- Long time with the same V, states will concentrate
- 64 bit key / state are too short

**Biased birthday state guessing attack**

1. precompute the 64-bit outputs that correspond to the most likely states
2. observe until any of them appears in the actual transmission
LTE reference architecture

Main blocks

- Evolved Packet Core (EPC)
- Evolved Universal Terrestrial Radio Access Network (E-UTRAN)
- IP multimedia subsystem (IMS) network
- Machine Type Communication (MTC)
- Home eNodeB (HeNB)
- non-3GPP access networks
- evolved packet data gateway (ePDG)
LTE reference architecture

Main blocks

- Evolved Packet Core (EPC)
4th generation cellular networks: LTE

LTE reference architecture

Main blocks

- Evolved Packet Core (EPC)
- Evolved Universal Terrestrial Radio Access Network (E-UTRAN)
LTE reference architecture

Main blocks
- Evolved Packet Core (EPC)
- Evolved Universal Terrestrial Radio Access Network (E-UTRAN)
- IP multimedia subsystem (IMS) network

4th generation cellular networks: LTE
LTE reference architecture

**Main blocks**
- Evolved Packet Core (EPC)
- Evolved Universal Terrestrial Radio Access Network (E-UTRAN)
- IP multimedia subsystem (IMS) network

**New entities**
- Machine Type Communication (MTC)
- Home eNodeB (HeNB)
- non-3GPP access networks
- evolved packet data gateway (ePDG)
4th generation cellular networks: LTE

LTE reference architecture

Main blocks
- Evolved Packet Core (EPC)
- Evolved Universal Terrestrial Radio Access Network (E-UTRAN)
- IP multimedia subsystem (IMS) network

New entities
- Machine Type Communication (MTC)
LTE reference architecture

Main blocks
- Evolved Packet Core (EPC)
- Evolved Universal Terrestrial Radio Access Network (E-UTRAN)
- IP multimedia subsystem (IMS) network

New entities
- Machine Type Communication (MTC)
- Home eNodeB (HeNB)
4th generation cellular networks: LTE

**LTE reference architecture**

- **Main blocks**
  - Evolved Packet Core (EPC)
  - Evolved Universal Terrestrial Radio Access Network (E-UTRAN)
  - IP multimedia subsystem (IMS) network

- **New entities**
  - Machine Type Communication (MTC)
  - Home eNodeB (HeNB)
  - non-3GPP access networks
LTE reference architecture

Main blocks
- Evolved Packet Core (EPC)
- Evolved Universal Terrestrial Radio Access Network (E-UTRAN)
- IP multimedia subsystem (IMS) network

New entities
- Machine Type Communication (MTC)
- Home eNodeB (HeNB)
- non-3GPP access networks
- evolved packet data gateway (ePDG)
Security in the LTE standard

4th generation cellular networks: LTE

Security features

LTE has been designed with the following enhanced security features wrt UMTS:

- new AKA for mutual authentication between the User Equipment (UE) and the Mobility Management Entity (MME)
- new key hierarchy
- new handover key management

Long term credentials

The long term credentials for a user $A$ are his/her International mobile subscriber identity (IMSI) id$A$ and his LTE secret key $k_A$. The pair $(id_A, k_A)$ is stored in the user owned Universal subscriber identity module (USIM) and in his/her Authentication center (AuC).
Security in the LTE standard

Security features

LTE has been designed with the following enhanced security features wrt UMTS:

- New AKA for mutual authentication between the User Equipment (UE) and the Mobility Management Entity (MME)
- New key hierarchy
- New handover key management

Long term credentials

The long term credentials for a user A are his/her International mobile subscriber identity (IMSI) \(id_A\) and his LTE secret key \(k_A\). The pair \((id_A, k_A)\) is stored in the user owned Universal subscriber identity module (USIM) and in his/her Authentication center (AuC).
Security in the LTE standard

<table>
<thead>
<tr>
<th>Security features</th>
</tr>
</thead>
<tbody>
<tr>
<td>LTE has been designed with the following enhanced security features wrt UMTS:</td>
</tr>
<tr>
<td><strong>new AKA</strong> for mutual authentication between the User Equipment (UE) and the Mobility Management Entity (MME)</td>
</tr>
</tbody>
</table>

Long term credentials for a user $A$ are his/her International mobile subscriber identity (IMSI) $id_A$ and his LTE secret key $k_A$. The pair $(id_A, k_A)$ is stored in the user owned Universal subscriber identity module (USIM) and in his/her Authentication center (AuC).
Security in the LTE standard

Security features

LTE has been designed with the following enhanced security features wrt UMTS:

- **new AKA** for mutual authentication between the User Equipment (UE) and the Mobility Management Entity (MME)

- **new key hierarchy**

Long term credentials

The long term credentials for a user A are his/her International mobile subscriber identity (IMSI) idA and his LTE secret key kA. The pair (idA, kA) is stored in the user owned Universal subscriber identity module (USIM) and in his/her Authentication center (AuC).
Security in the LTE standard

Security features

LTE has been designed with the following enhanced security features wrt UMTS:

- new AKA for mutual authentication between the User Equipment (UE) and the Mobility Management Entity (MME)
- new key hierarchy
- new handover key management mechanism

Long term credentials

The long term credentials for a user $A$ are his/her International mobile subscriber identity (IMSI) $id_A$ and his LTE secret key $k_A$. The pair $(id_A, k_A)$ is stored in the user owned Universal subscriber identity module (USIM) and in his/her Authentication center (AuC).
Security in the LTE standard

Security features

LTE has been designed with the following enhanced security features wrt UMTS:

* new AKA for mutual authentication between the User Equipment (UE) and the Mobility Management Entity (MME)

* new key hierarchy

* new handover key management mechanism

Long term credentials

The long term credentials for a user A are his/her International mobile subscriber identity (IMSI) \( \text{id}_A \) and his LTE secret key \( k_A \).

The pair \((\text{id}_A, k_A)\) is stored in the user owned Universal subscriber identity module (USIM) and in his/her Authentication center (AuC)
Overview of EPS Authentication and Key Agreement

EPS-AKA main steps

1. LTE mutual authentication between MME and UE
Overview of EPS Authentication and Key Agreement

EPS-AKA main steps

1. LTE mutual authentication between MME and UE
2. Non access stratum (NAS) KA negotiating mechanisms and establishing keys between MME and UE
Overview of EPS Authentication and Key Agreement

EPS-AKA main steps

1. LTE mutual authentication between MME and UE
2. Non access stratum (NAS) KA negotiating mechanisms and establishing keys between MME and UE
3. Access stratum (AS) KA negotiating mechanisms establishing keys between eNBs and UE (both for C- and U-plane).
LTE authentication protocol

1. Attach Request (IMSI, UE Network Capability, KSI, Kc, Kk, Kk')
2. Authentication Information Request (IMSI, SN ID, n, Network Type)
3. Authentication Information
   - Select an AV (e.g., AV f)
4. MME uses KAAKE (KAAKE t) to calculate additional keys
5. Request for auth info
6. Answer with auth info
7. Auth request
8. Auth response
9. Auth complete
10. Key derivation

HSS
- IMSI: Provisioned @AuC
- LTE K: Provisioned @AuC
- RAND: HSS generates
- SQN: HSS generates (increase)
### LTE authentication protocol

**Protocol steps**

1. **Attach request**

   **UE**
   - **Attach Request** (IMSI, UE Network Capability, K_{SAAME=7})

   **MME**
   - **Authentication Information Request** (IMSI, SN ID, n, Network Type)

   **HSS**
   - IMSI: Provisioned @AuC
   - LTE K: Provisioned @AuC
   - RAND: HSS generates
   - SCRN: HSS generates (increase)

2. **Request for auth info**

3. **Answer with auth info**

4. **Auth request**

5. **Auth response**

6. **Auth complete**

7. **Key derivation**

---

**Credentials:**

- **IMSI:** Factory Default
- **LTE K:** Factory Default
- **RAND:** HSS generates
- **SCRN:** HSS generates (increase)

---

**Key derivation process:**

- UE uses K_{SAAME} (K_{SAAME l}) to calculate additional keys
- MME uses K_{SAAME} (K_{SAAME l}) to calculate additional keys

---

**Network Security:**

Nicolà Laurenti | Cellular Networks Security | December 5, 2017
LTE authentication protocol

Protocol steps:

1. Attach request
2. Request for auth info
LTE authentication protocol

Protocol steps

1. Attach request
2. Request for auth info
3. Answer with auth info

Protocol steps:

1. **Attach request**
   - **UE** (User Equipment) sends an attach request to the **MME** (Mobility Management Entity) with the IMSI (International Mobile Subscriber Identity), UE (User Equipment) identity, and network capability.
   - **MME** sends an authentication information request to the **HSS** (Home Subscriber Server) with the IMSI, SN ID (Subscriber Number), and network type.

2. **Authentication Information Request**
   - **HSS** generates the authentication information (AV) and sends it to **MME**.
   - **MME** sends the AV to the **UE**.

3. **Authentication Information Answer (Authentication Vectors)**
   - **UE** selects an AV (e.g., AV n) and sends it to the **MME**.
   - **MME** generates the key derivation function (KDF) using the AV and sends it to the **HSS**.
   - **HSS** calculates the final key (KAsME) using the KDF and sends it to the **MME**.

4. **Auth Request**
   - **MME** sends the authentication request to the **HSS**.

5. **Auth Response**
   - **HSS** sends the authentication response to the **MME**.

6. **Auth Complete**
   - **MME** sends the authentication complete message to the **UE**.

7. **Key Derivation**
   - **UE** and **MME** use the KAsME to calculate additional keys needed for encryption and integrity check.
LTE authentication protocol

1. Attach request
2. Request for auth info
3. Answer with auth info
4. Auth request
LTE authentication protocol

1. Attach request
2. Request for auth info
3. Answer with auth info
4. Auth request
5. Auth response
4th generation cellular networks: LTE

LTE authentication protocol

1. Attach request
2. Request for auth info
3. Answer with auth info
4. Auth request
5. Auth response
6. Auth complete
4th generation cellular networks: LTE

LTE authentication protocol

**Protocol steps**

1. Attach request
2. Request for auth info
3. Answer with auth info
4. Auth request
5. Auth response
6. Auth complete
7. Key derivation

**Protocol steps**

1. **Attach request**
   - **UE** sends Attach Request (IMSI, UE Network Capability, K_{SIM}=7)
   - **MME** receives Attach Request and generates RAND
   - **HSS** generates AUTN, XRES, K_{ASME}

2. **Authentication Information Request**
   - **MME** sends Authentication Information Request (IMSI, SN ID, n, Network Type)
   - **HSS** generates AV = RAND1, AUTN1, XRES1, K_{ASME1}

3. **Authentication Information Answer**
   - **UE** selects an AV (e.g., AV 1)
   - **MME** verifies AUTN with K_{ASME1}
   - **HSS** authenticates UE if AUTN = AUTN_{UE}

4. **Authentication Request**
   - **UE** generates KDF(K_{ASME1})
   - **MME** uses K_{ASME} to derive K_{ASME1}

5. **Authentication Response**
   - **UE** sends Authentication Complete
   - **MME** encrypts XRES with K_{ASME}

6. **Key derivation**
   - UE uses K_{ASME} to generate additional keys (for Encryption & Integrity Check)

Nicola Laurenti
Cellular Networks Security
December 5, 2017
NAS and AS security negotiation

2. NAS Security Setup

- NAS Security Mode Command (KS_SAM = 1, Replayed UE Network Capability, NAS Ciphering Algorithm=EIA1, NAS Integrity Algorithm=EIA1, NAS-MAC)
  - [NAS integrity protected]

- NAS Security Mode Complete (NAS-MAC)
  - [NAS ciphered and integrity protected]

- Ciphered and Integrity Protected NAS Signaling

3. AS Security Setup

- AS Security Mode Command (Ciphering Algorithm=EIA1, Integrity Algorithm=EIA1, MAC-I)
  - [AS integrity protected]

- AS Security Mode Complete (MAC-I)
  - [AS integrity protected]

- Ciphered and Integrity Protected RRC Signaling

- Ciphered User Plane (Data Plane)
Key handover among eNBs

Motivation

$K_{eNB}$ should be unique for each eNB and known only by that specific base station.

- user’s mobility forces a change of the serving eNB.
- backward security: the new eNB does not know the previous $K_{eNB}$
- 2-step forward security: the old eNB knows the next $K_{eNB}$ but won’t know the following.

Handover techniques

A Next Hop key (NH) is used: unique for each eNB and delivered and updated by MME.

- Horizontal key derivation: obtain new $K_{eNB,t+1}^{t+1}$ by applying a one-way function to the old one: $K_{eNB,t+1}^{t+1} = h_\alpha(K_{eNB,t})$.
- Vertical key derivation: when a base station has a fresh NH key, it obtains the new $K_{eNB}$ as: $K_{eNB,t+1}^{t+1} = h_\alpha(NH)$. 
LTE key hierarchy

<table>
<thead>
<tr>
<th>Key</th>
<th>Period</th>
<th>Bits</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>K</td>
<td></td>
<td></td>
<td>Lifetime</td>
</tr>
<tr>
<td>CK, IK</td>
<td></td>
<td></td>
<td>Session</td>
</tr>
<tr>
<td>K_ASME</td>
<td></td>
<td></td>
<td>Session</td>
</tr>
<tr>
<td>K_NASenc</td>
<td></td>
<td></td>
<td>Session</td>
</tr>
<tr>
<td>K_NASint</td>
<td></td>
<td></td>
<td>Session</td>
</tr>
<tr>
<td>K_eNB</td>
<td></td>
<td></td>
<td>Handover</td>
</tr>
<tr>
<td>K_UPenc</td>
<td></td>
<td></td>
<td>Handover</td>
</tr>
<tr>
<td>K_RRCint</td>
<td></td>
<td></td>
<td>Handover</td>
</tr>
<tr>
<td>K_RRCenc</td>
<td></td>
<td></td>
<td>Handover</td>
</tr>
</tbody>
</table>

Nicola Laurenti
Cellular Networks Security
December 5, 2017
LTE key hierarchy

<table>
<thead>
<tr>
<th>Key</th>
<th>Period</th>
<th>Bits</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>$K_A$</td>
<td>lifetime</td>
<td>128</td>
<td>master</td>
</tr>
</tbody>
</table>
LTE key hierarchy

<table>
<thead>
<tr>
<th>key</th>
<th>period</th>
<th>bits</th>
<th>use</th>
</tr>
</thead>
<tbody>
<tr>
<td>$K_A$</td>
<td>lifetime</td>
<td>128</td>
<td>master</td>
</tr>
<tr>
<td>CK</td>
<td>session</td>
<td>128</td>
<td>encryption</td>
</tr>
<tr>
<td>IK</td>
<td>session</td>
<td>128</td>
<td>integrity</td>
</tr>
</tbody>
</table>

Nicola Laurenti
Cellular Networks Security
December 5, 2017
LTE key hierarchy

<table>
<thead>
<tr>
<th>key</th>
<th>period</th>
<th>bits</th>
<th>use</th>
</tr>
</thead>
<tbody>
<tr>
<td>$K_A$</td>
<td>lifetime</td>
<td>128</td>
<td>master</td>
</tr>
<tr>
<td>$CK$</td>
<td>session</td>
<td>128</td>
<td>encryption</td>
</tr>
<tr>
<td>$IK$</td>
<td>session</td>
<td>128</td>
<td>integrity</td>
</tr>
<tr>
<td>$K_{ASME}$</td>
<td>session</td>
<td>256</td>
<td>master</td>
</tr>
</tbody>
</table>
LTE key hierarchy

<table>
<thead>
<tr>
<th>key</th>
<th>period</th>
<th>bits</th>
<th>use</th>
</tr>
</thead>
<tbody>
<tr>
<td>$K_A$</td>
<td>lifetime</td>
<td>128</td>
<td>master</td>
</tr>
<tr>
<td>CK</td>
<td>session</td>
<td>128</td>
<td>encryption</td>
</tr>
<tr>
<td>IK</td>
<td>session</td>
<td>128</td>
<td>integrity</td>
</tr>
<tr>
<td>$K_{ASME}$</td>
<td>session</td>
<td>256</td>
<td>master</td>
</tr>
<tr>
<td>$K_{NAS,enc}$</td>
<td>session</td>
<td>256</td>
<td>NAS encrypt</td>
</tr>
<tr>
<td>$K_{NAS,int}$</td>
<td>session</td>
<td>256</td>
<td>NAS integrity</td>
</tr>
</tbody>
</table>
LTE key hierarchy

<table>
<thead>
<tr>
<th>key</th>
<th>period</th>
<th>bits</th>
<th>use</th>
</tr>
</thead>
<tbody>
<tr>
<td>$K_A$</td>
<td>lifetime</td>
<td>128</td>
<td>master</td>
</tr>
<tr>
<td>CK</td>
<td>session</td>
<td>128</td>
<td>encryption</td>
</tr>
<tr>
<td>IK</td>
<td>session</td>
<td>128</td>
<td>integrity</td>
</tr>
<tr>
<td>$K_{ASME}$</td>
<td>session</td>
<td>256</td>
<td>master</td>
</tr>
<tr>
<td>$K_{NAS,enc}$</td>
<td>session</td>
<td>256</td>
<td>NAS encrypt</td>
</tr>
<tr>
<td>$K_{NAS,int}$</td>
<td>session</td>
<td>256</td>
<td>NAS integrity</td>
</tr>
<tr>
<td>$K_{eNB}$</td>
<td>handover</td>
<td>256</td>
<td>master</td>
</tr>
</tbody>
</table>
LTE key hierarchy

<table>
<thead>
<tr>
<th>Key</th>
<th>Period</th>
<th>Bits</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>K_A</td>
<td>lifetime</td>
<td>128</td>
<td>master</td>
</tr>
<tr>
<td>CK</td>
<td>session</td>
<td>128</td>
<td>encryption</td>
</tr>
<tr>
<td>IK</td>
<td>session</td>
<td>128</td>
<td>integrity</td>
</tr>
<tr>
<td>K_{ASME}</td>
<td>session</td>
<td>256</td>
<td>master</td>
</tr>
<tr>
<td>K_{NAS,enc}</td>
<td>session</td>
<td>256</td>
<td>NAS encrypt</td>
</tr>
<tr>
<td>K_{NAS,int}</td>
<td>session</td>
<td>256</td>
<td>NAS integrity</td>
</tr>
<tr>
<td>K_{eNB}</td>
<td>handover</td>
<td>256</td>
<td>master</td>
</tr>
<tr>
<td>K_{RRC,enc}</td>
<td>handover</td>
<td>256</td>
<td>AS C-plane enc-</td>
</tr>
<tr>
<td>K_{RRC,int}</td>
<td>handover</td>
<td>256</td>
<td>AS C-plane int-</td>
</tr>
</tbody>
</table>
LTE key hierarchy

<table>
<thead>
<tr>
<th>key</th>
<th>period</th>
<th>bits</th>
<th>use</th>
</tr>
</thead>
<tbody>
<tr>
<td>$K_A$</td>
<td>lifetime</td>
<td>128</td>
<td>master</td>
</tr>
<tr>
<td>CK</td>
<td>session</td>
<td>128</td>
<td>encryption</td>
</tr>
<tr>
<td>IK</td>
<td>session</td>
<td>128</td>
<td>integrity</td>
</tr>
<tr>
<td>$K_{ASME}$</td>
<td>session</td>
<td>256</td>
<td>master</td>
</tr>
<tr>
<td>$K_{NAS,enc}$</td>
<td>session</td>
<td>256</td>
<td>NAS encrypt</td>
</tr>
<tr>
<td>$K_{NAS,int}$</td>
<td>session</td>
<td>256</td>
<td>NAS integrity</td>
</tr>
<tr>
<td>$K_{eNB}$</td>
<td>handover</td>
<td>256</td>
<td>master</td>
</tr>
</tbody>
</table>
| $K_{RRC,enc}$ | handover     | 256  | AS C-plane en-
|            |               |      | cription       |
| $K_{RRC,int}$ | handover     | 256  | AS C-plane in-
|            |               |      | terity         |
| $K_{UP,enc}$ | handover     | 256  | AS U-plane en-
|            |               |      | cription       |
Security at HeNB
Security in MTC

(a) MTC server is located in or outside the operator domain

(b) MTC Devices communicating directly with each other without intermediate MTC server
LTE vs UMTS network access

LTE

MME/S-GW

HeNB-GW

X2

eNB

UMTS

SGSN/GGSN

RNC

cNB

HeNB

Nicola Laurenti

Cellular Networks Security

December 5, 2017 20 / 22
Handover to non 3-GPP access
Further references

G. M. Koien
“An introduction to access security in UMTS”

J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo
“A Survey on Security Aspects for LTE and LTE-A Networks”

NMC Consulting Group Co.
*LTE Security I — Security Concept and Authentication*

NMC Consulting Group Co.
*LTE Security II — Security Concept and Authentication*

Dan Forsberg, Gnther Horn, Wolf-Dietrich Moeller, Valtteri Niemi
*LTE Security*